BUILDING BLOCK

MOBILE DEVICE SECURITY FOR ENTERPRISES

Working Draft, Not for Distribution
May 8, 2014
mobile-nccoe@nist.gov

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) works with industry, academic and government experts to find practical solutions for businesses' most pressing cybersecurity needs. The NCCoE collaborates to build open, standards-based, modular, end-to-end solutions that are broadly applicable, customizable to the needs of individual businesses, and help businesses more easily comply with applicable standards and regulations.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a community of interest including vendors of cybersecurity solutions. The solution will become an NCCoE "Building Block": an approach that can be incorporated into multiple use cases. The solution proposed by this effort will not be the only one available in the fast-paced cybersecurity technology market. If you would like to propose an alternative architecture or know of products that might be applicable to this challenge, please contact us at mobile-nccoe@nist.gov.

1. DESCRIPTION

Goal

Traditionally, enterprises have established a boundary to separate their trusted internal network(s) from untrusted external networks. The consumption and generation of corporate information on mobile devices erodes this traditional boundary. Faced with a rapidly changing array of mobile platforms, corporations must ensure that mobile devices connected to the enterprise can be trusted to protect sensitive corporate data as it is stored, accessed or processed on the device, without compromising the end user's experience.

This building block will demonstrate commercially available technologies that provide enterprise-class protection to both organization-issued and personally-owned mobile platforms. These technologies enable users to work inside and outside the corporate network with a securely configured mobile device, while allowing for granular control over the enterprise network boundary, and minimizing the impact on function. The architecture demonstrated by this building block will incorporate a layered technology stack that allows enterprises to tailor solutions to their business needs.

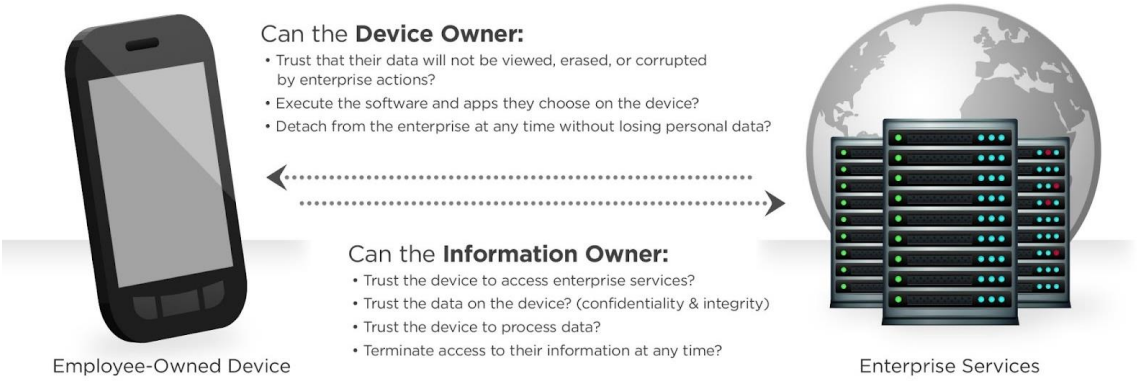
Background

In the past decade, mobile devices have significantly changed business capabilities, allowing employees access to information resources wherever they are, whenever they need to. These capabilities pose both an opportunity and a challenge. While their always-on, always-connected nature can make business practices more efficient and effective, mobile devices create new challenges to ensure the confidentiality, integrity and availability of information they access.

As these technologies mature, employees increasingly want to use both corporate-issued and personally-owned mobile devices to access corporate enterprise services, data and resources to perform work-related activities. Enterprises are under pressure to accept the associated security risks inherent in today's mobile devices because of several factors, including anticipated cost savings and employees' desire for greater convenience.

2. SCENARIOS

This building block will demonstrate security capabilities that can provide greater assurance that a mobile device can be trusted to protect data stored, accessed or processed on the device. Understanding that every organization makes decisions regarding access to its resources based on an analysis of its enterprise risk posture, these solutions envision tools that support an array of security controls. To ensure that these security controls realize their maximum effectiveness, this build block will address the usability and security expectations of both the employee and the enterprise.



Scenario: The User Perspective

A new employee would like to access corporate information resources, namely her e-mail, calendar, contacts and files from a mobile device (e.g., smart phone or tablet). Upon request, the employee is informed that her company can either provision her personal device or provide her with a preconfigured device procured by the company. The inconvenience of carrying around an extra mobile device does not appeal to her but she also knows that using a single device for both her personal life and work requires her company to implement certain device restrictions in order to protect the corporate data she will be accessing.

At the employee's prior company, mandatory policies severely diminished her ability to use the device. Unlocking the device required long passwords, which she often mistyped. Each time she accessed corporate files she had to set up a secure connection, requiring yet another password. Without warning, the company blacklisted a banking application she used to deposit her paychecks. If the company detected malware on her device she had to give it to the IT staff, who would keep it for a week to remediate the incident.

Leary of repeating her prior experience, she decides to talk with the IT staff about what restrictions the company might put on device usage. The IT staff informed her that company security controls are designed to minimize the impact on the user. The company would logically separate personal and corporate data and applications on the device, protected by password-based authentication. Remote access requires a protected tunnel back to the enterprise, but once she is authenticated to access her corporate profile she can activate the protected connection with a single touch. Remote authentication is handled without user interaction via the use of digital certificates.

After initial configuration, notifications would be sent directly to the device to inform her of any upcoming policy changes, such as restricted applications, prior to the policy being remotely pushed. Her company would have to monitor the device for security incidents and malicious behavior, however monitoring would be limited to the logical areas storing corporate data. In the event that her device was infected by malware, it would be quarantined from enterprise resources automatically, allowing her to maintain the device for personal use. She would then have the option to allow her company to perform remote remediation procedures on the device, prior to regaining access to enterprise resources.

If, at any time, the employee needs to perform actions that are restricted by the corporate policy, she can revoke her own access to the corporate services and information. To re-enroll, her device will need to undergo a health check to ensure that it is in a known good state and the security architecture is not compromised.

With a thorough understanding of the security controls and usability considerations, she now must decide which solution best fits her needs.

Scenario: The Enterprise Perspective

Facing increasing demand from employees to access sensitive data on mobile devices, an enterprise decides to implement a new mobile security strategy. In the past, the enterprise provided users with secured mobile devices; however, the restrictions placed on the devices encumbered the user and system management required significant IT resources to keep up with device provisioning, maintenance and security remediation. Any new strategy needs to provide modern security and asset management capabilities while easily integrating with current production systems.

Prior to device enrollment, the corporate IT staff will perform a remote scan to determine the current health and integrity of the device. Once the device is deemed acceptable, the enterprise will enroll the device by remotely pushing user and device specific security policies. Policy implementation allows the enterprise to maintain a logical separation between corporate and user data. Cryptographic tokens for accessing enterprise email and other resources are also remotely delivered to ensure encryption mechanisms are properly used once the employee receives the device.

Once users are allowed to access enterprise resources, it should be easy to maintain an asset database and push policy and system updates to all enrolled devices. Compliance checks should occur automatically on regular intervals, with policy violations immediately reported to the employee and the enterprise for remediation. For audit purposes, regular scanning and logging should occur automatically and be reported back to the enterprise. For security incident triaging and remediation, the security dashboard should easily display pertinent audit and logging information and enable the enterprise to cut off resources and/or remotely wipe corporate data from the malicious device.

With these expectations in mind, the enterprise can draft and implement the new mobile strategy.

3. Architecture Characteristics

Specific methods for meeting both user and enterprise expectations require the implementation of both usability and security characteristics. Figure 1 demonstrates the relationship between usability and security in the mobile device space.

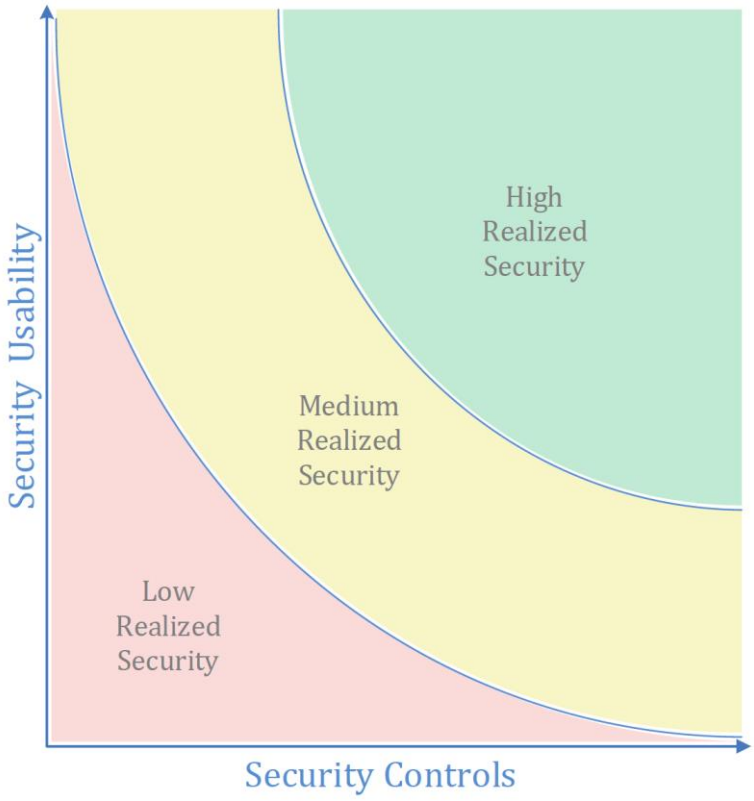


Figure 1. The relationship between security and usability.

Expectations that mobile devices should support both personal and enterprise uses has given rise to the "consumer enterprise." When securing these devices, the usability expectations of both the enterprise and user must be taken into consideration. An increase in security controls alone does not guarantee an increase in security. Instead,

the proper implementation of usable security controls results in an enterprise mobile security posture that protects corporate data without encumbering the user.

The characteristic sets found below are considered attributes of a secure solution. Each characteristic has one or more examples of a capability that would meet the intent of the characteristic. These characteristics and corresponding capabilities are not exhaustive. Furthermore, capabilities are defined to provide context for the characteristics and are not meant to be prescriptive.

Security Characteristics

All characteristics should be implemented with verifiable integrity via continued assertions that the device has not been compromised (e.g., that key firmware or operating system files have not been tampered with, that the device has not been "rooted" or "jail broken," and that the device's security policies are verified as those being issued by the enterprise).

Security characteristics	Example security capabilities
data protection	• protected storage - secure containers - device encryption - trusted key storage - hardware security modules - remote wipe: render access to corporate data stored on the device infeasible • protected communications - VPN, to include per-app VPN • data protection in process - encrypted memory - protected execution environments
data isolation	• virtualization • sandboxing • memory isolation • device resource management: ability to enable/disable device peripherals • data flow control - data tagging: as data is accessed by a mobile application, policies relevant to that data are transmitted simultaneously and enforced on that data by the application • baseband isolation: ensure that the device, operating system and applications are communicating with the baseband network in a deterministic matter

Table continues, next page

Security characteristics	Example security capabilities
device integrity	• baseband integrity checks: ensure that the baseband operating system has not been tampered with • application black/whitelisting • device integrity checks: - boot validation: validation the that device is in a known working state and untampered with at boot; e.g. bios integrity checks - application verification: ensure corporate applications being installed come from a valid source - verified application and OS updates - trusted integrity reports: ensure that integrity reports pulled from the device are representative of the current and true state of the device - policy integrity verification: ensure that the policies received by the device come from a verified source
monitoring	• canned reports and ad-hoc queries • auditing and logging: capture and store device and application information • anomalous behavior detection: observe activities of mobile users, devices and processes, and measure those activities against a baseline of known normal activity • compliance checks: provide information about whether a device has remained compliant with a mandated set of policies • asset management • root and jailbreak detection: ensure that the security architecture for a mobile device has not been compromised • geo-fencing: monitor a device's geolocation and enable/disable device and network resources based on that location
identity and authorization	• authentication of user - local authentication to applications - local authentication to device - remote authentication • authentication of device - remote authentication • implementation of user and device roles for authorization • credential and token storage and use • device provisioning

Usability Characteristics

Turning theoretical security controls into real world security requires system security designs that meet the usability expectations of both the employee and the enterprise. The usability characteristics and capabilities below are examples of usability considerations that greatly affect realized security within an enterprise mobility management strategy.

132

Usability characteristics	Example usability capabilities	Usability benefactor
provisioning	• ability to provision the device remotely	user and enterprise
software update management	• remote application delivery and updates: push application and OS patches, as well as new applications, to the device • remote system updates: distribute the newest releases of corporate applications and security software	user and enterprise
policy management	• remotely push new or updated policies to the device • notify users of any expected functionality changes prior to the update	user and enterprise
monitoring	• automatic regular integrity and compliance checks on the device • automated alerts for policy violations	enterprise
audit	• automatically generate reports/dashboard for auditing • easy to access and interpret logging	enterprise
unobtrusive remediation procedures	• should a device compromise occur, security incident remediation can be performed with little to no loss of personal functionality on the device	user
unobtrusive protected connection establishment	• ability for the user to quickly and easily establish a protected connection between the device and the corporate resources	user
unobtrusive authentication methods	• authentication to applications and services done in the background without the need for user interaction	user
privacy protection	• company should not be able to monitor personal activity or capture personal information such as non-corporate account authentication credentials	user
simple key management	• the ability to easily obtain keys for encrypted e-mail	user
secure file sharing	• drag-and-drop secure file transfer and sharing	user

133 ## 4. APPROACH

134 This building block demonstrates a commercially available set of technology that
135 addresses the security challenges that mobile devices present to an enterprise. This
136 project will take a “device up” approach, starting with the implementation of security
137 characteristics and capabilities that involve the mobile device and its management.
138 Figure 2 demonstrates example capabilities that fit into the device technology stack.

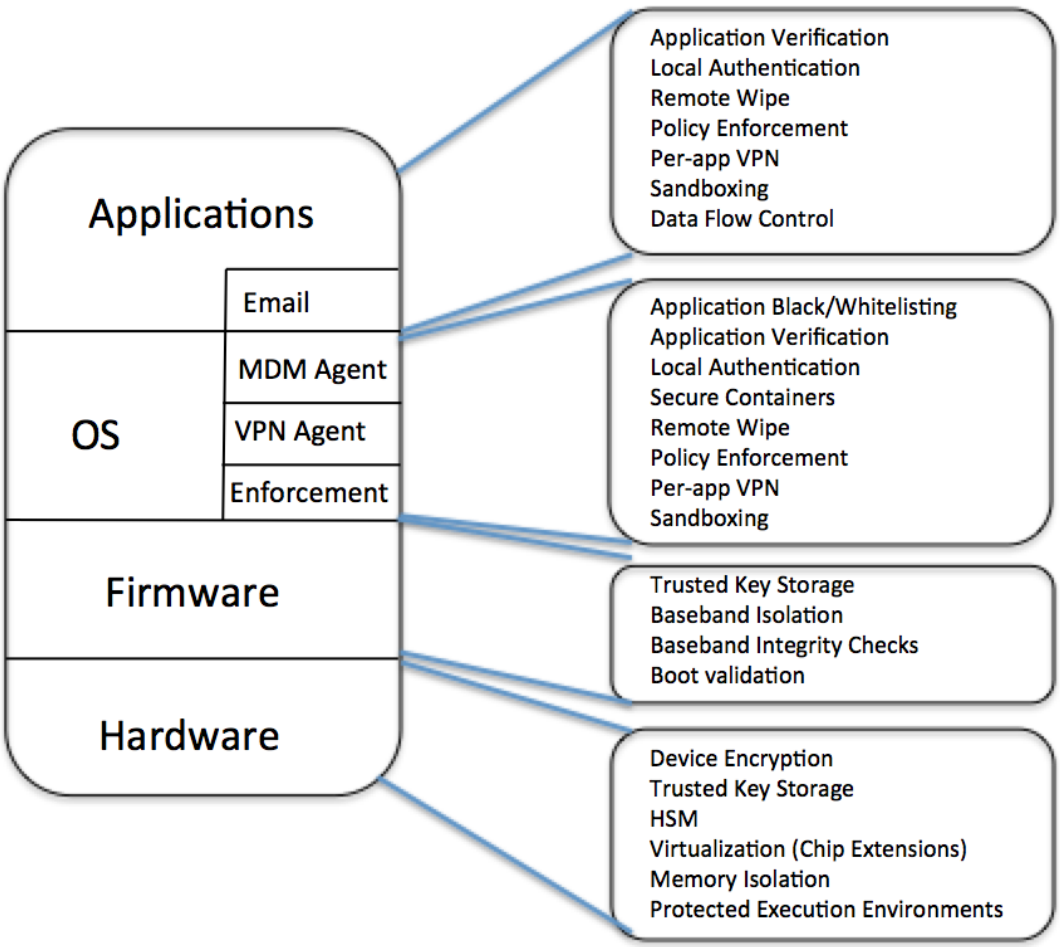


Figure 2. High-level device architecture

The implementation of device security capabilities that leverage an enterprise mobility management suite (EMM), will necessitate that the build evolve to include an enterprise mobility security architecture. The architecture will demonstrate that the hardened mobile device can securely access corporate data for which the user and device are authorized and that accessed data stays within corporately defined boundaries and terms of use. Throughout the build process, the implementation of all security characteristics shall be mapped to their applicable security controls found in the standards in Section 6 of this document.

In order to address a full array of mobile platforms and technologies, several initial builds may occur as part of this building block. Note that this is an initial approach and that the building block process is intended to be iterative. As mobile technologies and capabilities evolve, the initial technology set of this building block may be augmented with additional functionality.

5. Business Value

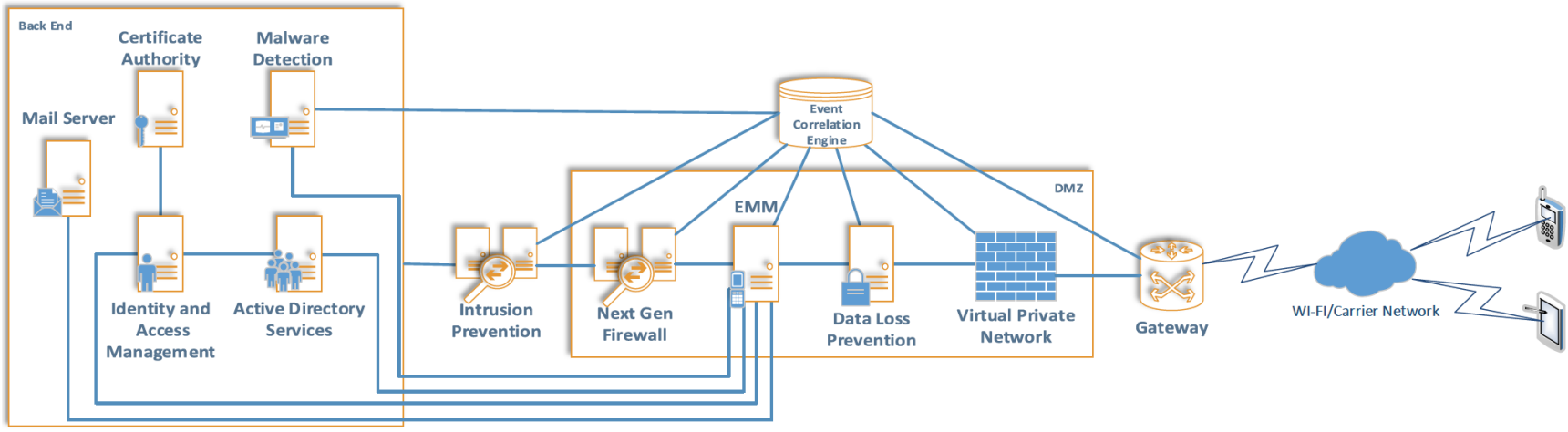
- provides enterprise-class protection to users who need to access untrustworthy cellular and Wi-Fi networks, peripherals, apps and web sites
- enables users to work inside and outside the corporate network with a hardened mobile device that is unlikely to adversely affect an enterprise
- reduces total outlays in redundant enterprise network security systems by improving security of mobile devices
- helps companies embrace the BYOD model and reduce corresponding capital investment by increasing security on users' mobile devices
- broadens visibility of users' behavior in accessing and working on corporate networks in order to bolster identity and access management capabilities

6. Relevant Standards

- NIST SP 800-124 Rev 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-164, Guidelines on Hardware-Rooted Security for Mobile Devices
- Global Platform Secure Element and Trusted Execution Environment Specifications
- Trusted Computing Group Trusted Platform Module and Trusted Network Connect Specifications
- NIST SP 800-147: BIOS Protection
- NIST SP 800-155: BIOS Integrity Measurements
- NSA Mobility Capability Package 2.2
- DoD Mobility Implementation Plan
- NIAP Protection Profile for Mobile Device Management Systems
- NIAP Protection Profile for Mobile Devices
- NIAP Protection Profiles for Virtual Private Networks
- Digital Government Strategy Mobile Security Baseline
- GSA Managed Mobility Program Request for Technical Capabilities

7. HIGH-LEVEL ARCHITECTURE

The high-level architecture depicts an example enterprise mobility management solution implemented within an enterprise.



8. COMPONENT LIST

- an initial set of mobile devices:
  - Samsung Galaxy XIV
  - Samsung Tab II + III
  - iPad & iPhone on iOS7
  - Surface Pro II (Pro + RT)
  - Dell venue Pro II (Core & Atom)
  - Nokia 1020 & 1520
- mobile devices (e.g., smartphone, tablet) with hardware security features outlined in NIST SP 800-164
- enterprise mobility management suite
- mobile applications requiring security assurance
  - e.g. applications that can be put in a secure container, allow for wrapping, etc…
- identity and access management system
- data loss prevention (DLP) solution
- event correlation engine
- enterprise infrastructure (e.g., directory server, VPN gateways, internal network, certification authority)